UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/929,476	08/13/2001	Luu Tran	SUN-P6088	9070

32615 7590 07/14/2005

OSHA LIANG L.L.P./SUN
1221 MCKINNEY, SUITE 2800
HOUSTON, TX 77010

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 07/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/929,476	TRAN ET AL.	
	Examiner	Art Unit	
	Jeffrey D. Popham	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5 and 7-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5 and 7-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 April 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Remarks

Claims 1-5 and 7-26 are pending.

Response to Arguments

1. Applicant's arguments, see applicant's remarks, filed 4/13/2005, with respect to the rejection(s)of claim(s) 1-26 under 35 U.S.C. 102 and 103 have been fully considered and are persuasive. Therefore, the rejections have been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Dusse (U.S. Patent Application Publication 2002/0,068,554), PAM (Samar, "Unified Login with Pluggable Authentication Modules (PAM)", 1996, pp. 1-10, obtained from http://portal.acm.org/citation.cfm?id=238177&coll=ACM&dl=ACM&CFID=48199134&CFTOKEN=38109131), Liao et al. (U.S. Patent 6,606,663), and iPlanet (Sun Microsystems, "iPlanet Portal Server Administrator Guide, Chapter 6 (Managing Authentication)", 5/4/2000, pp. 1-24, obtained from http://docs.sun.com/source/816-6128-10/authctn.htm).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-5, 7, 8, 15, 16, and 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dusse (U.S. Patent Application Publication 2002/0,068,554) in view of PAM (Samar, "Unified Login with Pluggable Authentication Modules (PAM)", 1996, pp. 1-10, obtained from http://portal.acm.org/citation.cfm?id=238177&coll=ACM&dl=ACM&CFID=48199134&CFTOKEN=38109131).

Regarding Claim 1,

Dusse discloses a client aware authentication system in a wireless network, comprising:

A wireless network (Page 4, Paragraph 47);

A plurality of classes of wireless clients, each of the classes of wireless clients having unique authentication parameters (Page 2, Paragraph 26; and Page 3, Paragraphs 36-37); and

An authentication service that selectively provides client specific authentication information to authenticate the plurality of classes of wireless clients using the unique authentication parameters (Page 4, Paragraph 47);

But does not disclose a plurality of authentication modules within this authentication service.

PAM, however, discloses a plurality of authentication modules within an authentication service [PAM API] (Pages 2-3, Section 3; and Figure 1). It would have been obvious to one of ordinary skill in the art at

the time of applicant's invention to incorporate the pluggable authentication module system of PAM into the wireless authentication system of Dusse in order to provide for authentication modules to be switched out, modified, and added as needs and security concerns change, as well as allowing ease of use for both users and administrators (Page 1, Section 1).

Regarding Claim 2,

PAM discloses that the plurality of authentication modules are coupled to an authentication service and wherein the authentication service is for dynamically selecting an authentication service module based on the class of a client (Pages 2-3, Section 3; and Figure 1). The different client types are the applications that connect to the authentication service (ex. ftp, telnet, login) with the authentication modules being specified for each one in the configuration file of table 1.

Regarding Claim 3,

Dusse discloses that the authentication service receives and parses client type information of the wireless clients to determine authentication characteristics of the wireless clients (Page 4, Paragraph 47).

Regarding Claim 4,

PAM discloses that the plurality of authentication modules comprises a set of predefined authentication parameters used by the

server to authenticate the wireless clients with known authentication characteristics accessing the server (Pages 4-5, Section 7.1) and Dusse discloses that it is a wireless server (Page 4, Paragraph 47).

Regarding Claim 5,

PAM discloses that the plurality of authentication modules further comprises authentication parameters dynamically extracted from client type information of the clients accessing the server (Pages 4-5, Section 7.1) and Dusse discloses that the clients and server are wireless (Page 2, Paragraph 26; and Page 4, Paragraph 47).

Regarding Claim 7,

Dusse discloses a wireless server system, comprising:

Wireless clients (Page 2, Paragraph 26);

A wireless server (Page 4, Paragraph 47); and

An authentication service, in response to receiving a particular client type associated with a particular wireless device, for authenticating the client (Page 4, Paragraph 47);

But does not disclose a plurality of authentication modules each providing respective authentication parameters pertinent to a type of client, the fact that the authentication service dynamically selects an authentication module based on the particular client type, or that the authentication service is also for applying a selected authentication module to the particular device for the authentication thereof.

PAM, however, discloses a plurality of authentication modules each providing respective authentication parameters pertinent to a type of client (Pages 2-3, Section 3; and Figure 1); and

An authentication service for dynamically selecting an authentication module of the plurality of authentication modules based on the particular client type (Pages 2-3, Section 3; and Figure 1);

Wherein the authentication service is also for applying a selected authentication module to the particular device for the authentication thereof (Pages 2-3, Section 3; and Figure 1).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the pluggable authentication module system of PAM into the wireless authentication system of Dusse in order to provide for authentication modules to be switched out, modified, and added as needs and security concerns change, as well as allowing ease of use for both users and administrators (Page 1, Section 1).

Regarding Claim 8,

Dusse discloses an automatic client detection service for automatically detecting the particular client type in response to service requests that originate from the particular wireless device (Page 3, Paragraphs 36-37).

Regarding Claim 15,

Dusse discloses a wireless server, comprising:

A client aware authentication service logic (Page 4, Paragraph 47);

A client data storage module for storing client type information (Page 3, Paragraph 37); and

Wireless clients (Page 2, Paragraph 26);

But does not disclose a plurality of client aware authentication modules, wherein the plurality of client aware authentication modules selectively provide client specific authentication information to authenticate a plurality of clients using unique authentication parameters or a session service module for storing transient session information for a client requesting authentication to the server.

PAM, however, discloses a plurality of client aware authentication modules, wherein the plurality of client aware authentication modules selectively provide client specific authentication information to authenticate a plurality of clients using unique authentication parameters (Pages 2-3, Section 3; and Figure 1); and

A session service module for storing transient session information for a client requesting authentication to the server (Pages 2-3, Section 3; and Figures 1 and 2).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the pluggable authentication module system of PAM into the wireless authentication system of Dusse in order to provide for authentication modules to be switched out, modified,

and added as needs and security concerns change, as well as allowing ease of use for both users and administrators (Page 1, Section 1).

Regarding Claim 16,

Dusse discloses that the authentication service logic authenticates clients attempting to access the wireless server (Page 4, Paragraph 47).

Regarding Claim 24,

Dusse discloses wireless clients (Page 2, Paragraph 26) and a wireless server (Page 4, Paragraph 47), but does not disclose a client aware authentication module comprising a plurality of client aware characteristics modules, wherein the plurality of client aware characteristics modules provide client specific authentication information in order to authenticate a plurality of clients access a server.

PAM, however, discloses a client aware authentication module, comprising:

A plurality of client aware characteristics modules, wherein the plurality of client aware characteristics modules provide client specific authentication information in order to authenticate a plurality of clients access a server (Pages 2-3, Section 3; and Figure 1); and

Client aware authentication selection logic (Pages 2-3, Section 3; and Figure 1).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the pluggable authentication

module system of PAM into the wireless authentication system of Dusse in order to provide for authentication modules to be switched out, modified, and added as needs and security concerns change, as well as allowing ease of use for both users and administrators (Page 1, Section 1).

Regarding Claim 25,

PAM discloses that the plurality of client aware characteristics modules comprise predefined set of client characteristics for authenticating clients access the client aware authentication module (Pages 4-5, Section 7.1).

Regarding Claim 26,

PAM discloses that the plurality of client aware characteristics modules comprise client characteristics dynamically extracted from the client run-time environment (Pages 4-5, Section 7.1).

3. Claims 9-12 and 17-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dusse in view of PAM, further in view of Liao et al. (U.S. Patent 6,606,663).

Regarding Claim 9,

Dusse as modified by PAM does not disclose that the service requests comprise header information which is used to detect the particular client type.

Liao, however, discloses that the service requests comprise header information which is used to detect the particular client type (Column 2, lines 18-35; and Column 7, lines 7-61). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the wireless system headers of Liao into the wireless authentication system of Dusse as modified by PAM in order to obtain the client's credentials so as to allow for proper authentication of the device.

Regarding Claim 10,

Liao discloses that the header information comprises HTTP headers (Column 2, lines 18-35; and Column 7, lines 7-61).

Regarding Claim 11,

Dusse discloses programmable user specific information within the authentication information transmitted to the server (Pages 3-4, Paragraphs 37 and 47).

Liao discloses that the authentication information is transmitted to the server in an authentication credential stored within the headers (Column 2, lines 18-35; and Column 7, lines 7-61).

Regarding Claim 12,

Dusse discloses that the authentication information comprises equipment manufacturer specified information [device ID] (Pages 3-4, Paragraphs 37 and 47).

Liao discloses that the authentication information is transmitted to the server in an authentication credential stored within the headers (Column 2, lines 18-35; and Column 7, lines 7-61).

Regarding Claim 17,

Dusse discloses that the authentication service logic retrieves client type information from the client data storage module and stores the client type information in the session service module to enable the client to be authenticated by the wireless server (Pages 3-4, Paragraphs 37 and 47). In order to authenticate/verify the user and device, the server of Dusse must retrieve the client type information from the client data storage module.

Regarding Claim 18,

PAM discloses that the authentication modules comprise a set of predefined authentication parameters for authentication known classes of clients that access the server (Pages 4-5, Section 7.1) and Dusse discloses that clients and server are wireless (Page 2, Paragraph 26; and Page 4, Paragraph 47).

Regarding Claim 19,

PAM discloses that the authentication modules comprise a set of dynamically extracted authentication parameters (Pages 4-5, Section 7.1), but Dusse as modified by PAM does not disclose that the authentication

parameters are send to the authentication service via service request headers.

Liao, however, discloses that authentication parameters are sent to the authentication service via service request headers (Column 2, lines 18-35; and Column 7, lines 7-61). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the wireless system headers of Liao into the wireless authentication system of Dusse as modified by PAM in order to obtain the client's credentials so as to allow for proper authentication of the device.

Regarding Claim 20,

PAM discloses that the authentication modules comprise selection logic to selectively choose authentication parameters in response to a client service request (Page 7, Section 11).

Regarding Claim 21,

Liao discloses that the client service request comprises HTTP request headers (Column 2, lines 18-35; and Column 7, lines 7-61).

Regarding Claim 22,

Dusse discloses that the authentication information comprises equipment manufacturer specified information [device ID] (Pages 3-4, Paragraphs 37 and 47).

Liao discloses that the authentication information is transmitted to the server in an authentication credential stored within the headers (Column 2, lines 18-35; and Column 7, lines 7-61).

Regarding Claim 23,

Dusse discloses programmable user specific information within the authentication information transmitted to the server (Pages 3-4, Paragraphs 37 and 47).

Liao discloses that the authentication information is transmitted to the server in an authentication credential stored within the headers (Column 2, lines 18-35; and Column 7, lines 7-61).

4. Claims 13 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dusse in view of PAM, further in view of iPlanet (Sun Microsystems, "iPlanet Portal Server Administrator Guide, Chapter 6 (Managing Authentication)", 5/4/2000, pp. 1-24, obtained from http://docs.sun.com/source/816-6128-10/authctn.htm).

Regarding Claim 13,

PAM discloses that the plurality of authentication modules comprises:

A user identification module (Pages 2-3, Section 3; and Figure 1);

A password module (Pages 2-3, Section 3; and Figure 1);

A membership module [different authentication modules for each role/membership that the user has] (Pages 4-5, Section 7.1);

A S/key module (Pages 2-3, Section 3; and Figure 1); and

A nopassword module [biometrics] (Page 2, Section 2);

But does not disclose securID, safeword, or Microsoft Windows/NT modules.

iPlanet, however, discloses:

A securID module (Pages 1-2; and Pages 16-17);

A safeword module (Pages 1-2; and Pages 15-16);

A Microsoft Windows/NT module (Pages 1-2; and Pages 13-15); and

A membership module (Pages 1-2).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication modules of iPlanet into the wireless authentication system of Dusse as modified by PAM because PAM discloses using any authentication mechanism as a module within the system in order to increase the extensibility of the system (PAM, Page 1, Section 1; and Page 4, Sections 6 and 7).

Regarding Claim 14,

PAM discloses that the plurality of authentication modules further comprise a UNIX authentication module (Pages 2-3, Section 3; and Figure 1), but does not disclose RADIUS or LDAP authentication modules.

iPlanet discloses an LDAP authentication module (Pages 1-2; and Pages 9-11) and a RADIUS authentication module (Pages 1-2; and Pages 17-18).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137